REMARKS

Claim Status

Claims 1-32 are now pending, with claims 1 and 32 being in independent form. Claim 33 has been canceled. Claim 1 has been amended. No new matter has been added. Reconsideration of the application, as herein amended, is respectfully requested.

Overview of the Office Action

Claims 1-31 stand rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Publication No. 2002/0129247 ("*Jablon*") in view of U.S. Patent No. 5,867,577 ("*Patarin*"), and further in view of EP 0 325 238 ("*Yeda*").

Claims 32 stands rejected under 35 U.S.C. §103(a) as unpatentable over *Jablon* in view of *Patarin*, and further in view of U.S. Publication No. 2003/0182554 ("*Gentry*") and *Yeda*.

Applicant notes the Examiner has indicated that the latter rejection is directed to claim 32. However, "the use of public parameters exclusively to verify the authentication results" was formerly recited in independent claim 33. In view of the cancellation of independent claim 33, this rejection is moot.

Moreover, the Examiner has failed to otherwise indicate that claim 32 has been rejected. Applicant therefore maintains that independent claim 32 patentably defines over the cited art.

Applicant has carefully considered the Examiner's rejections and the comments provided in support thereof. For the following reasons, Applicant respectfully asserts that all claims now presented for examination in the present application are patentable over the cited art.

Patentability of the Independent Claim 1 Under 35 U.S.C. §103(a)

Independent claim 1 has been amended to clarify that more than one parameter is calculated prior to the transaction and to clarify the relationship between a calculated parameter and a corresponding pseudo-random number r. Thus, independent claim 1 now recites "calculating, at the application prior to the transaction, parameters x corresponding to the at least one pseudo-random number r, each corresponding parameter x being linked to the pseudo-random number r by a mathematical relationship". Independent claim 1 also recites, *inter alia*, the steps of "producing a pseudo-random number r at the application", "producing, at the chip, the pseudo-random number r specific to the transaction via a serial pseudo-random generator included in the chip", "sending from the chip to the application the corresponding parameter x calculated by the application prior to the transaction", "calculating, at the chip, a parameter y constituting an entire or a portion of the authentication value V via a serial function", and the step of "verifying, at the application, said authentication value V via a verification function whose input parameters consist of public parameters including at least a public key p". The Examiner-applied combination of cited art fails to teach or suggest these express recitations of independent claim 1.

Jablon relates to a method for authenticating one party to the other using a series of messages that are exchanged over an open, insecure network, where interception or modification of the messages by an un-trusted third party may be possible (see Abstract). *Jablon* (paragraph [0040]) describes the establishment of "a large mutually-authenticated shared secret key between parties over an open insecure channel, where the authentication is based solely on mutual possession of a potentially small shared secret, such as a password".

As described at paragraph [0057] of *Jablon*, a pair of entities, i.e., Alice and Bob, "alone share knowledge of a secret password S". Bob proves his identity to Alice by proving his

knowledge of the result of a key exchange protocol, which is determined by parameters set according to a function of S". This exchange is known in the art as a simple password-authenticated exponential key exchange (SPIKE).

In contrast, the claimed invention is directed to an asymmetrical cryptographic method for protecting a hard-wired electronic logic chip against fraud in transactions between the electronic chip and an application. Consequently, the claimed invention provides an asymmetrical pair of keys comprised of a private key s and a public key p. In addition, performance of the calculation of an authentication value V occurs within the electronic chip using input parameters that include a random number r. *Jablon* simply fails to teach or suggest the claimed invention.

With reference to Fig. 1, *Jablon* teaches that Q_A is computed by Alice at step 104, which is part of a sequence comprised of steps 103, 104 and 106, where the computed Q_A is then sent to Bob (see paragraph [0066]). Applicant's independent claim 1 recites the step of "producing, at the chip, the pseudo-random number r specific to the transaction via a serial pseudo-random generator included in the chip". *Jablon* fails to teach or suggest this limitation. Independent claim 1 additionally recites that the pseudo-random generator is "included in the chip"; the pseudo-random random number r is thus produced locally in the chip via the pseudo-random generator. In *Jablon*, however, the value of the random number R_A is chosen from between 1 and N, and N is actually known by Bob. Moreover, *Jablon* teaches that the random number calculated at Bob is R_B, which differs from R_A. *Jablon* thus fails to teach or suggest this claimed step of applicant's independent claim 1.

Independent claim 1 further recites the step of "sending from the chip to the application the parameter x calculated by the application prior to the transaction, which is linked to the pseudo-random number r by the mathematical relationship and stored in the data memory of the chip".

Jablon also fails to teach or suggest this claimed step.

With further reference to Fig. 1 of *Jablon,* assuming *arguendo* that Q_A corresponds to parameter x (recited in independent claim 1) that would be sent to Bob, where $Q_A=H_{RA}(g)$, *Jablon* would still fail to teach or suggest applicant's claimed invention as recited in independent claim 1. Independent claim 1 defines that at least one parameter x is calculated by the application and is stored in the electronic chip prior to the performance of a transaction. In *Jablon*, the parameter Q_A is not calculated by Bob prior to a transaction. Consequently, *Jablon* does not provide a pre-transaction calculation that provides a parameter x that was stored or could have been stored in an internal memory of Alice (e.g., the chip with continued reference to this construct). *Jablon* thus fails to teach or suggest the subject matter of independent claim 1.

Independent claim 1 additionally recites the step of "calculating, at the chip, a parameter y constituting an entire or a portion of the authentication value V via a serial function whose input parameters are at least the random number r specific to the transaction and a private key s belonging to an asymmetrical pair of keys". *Jablon* also does not teach or suggest this step.

Jablon teaches that Alice (e.g., the chip) calculates a parameter constituting the entire or a portion of the authentication value V. *Jablon* (paragraph [0068]) teaches that "After Alice receives Q_B from Bob 125, Alice computes $K=H_{RA}(Q_B)$ 105". *Jablon* (paragraph [0076]) additionally explains that "Alice constructs the proof 107, sends this proof in a message V_A to Bob 108, and Bob verifies the proof 127 against his known value for K". *Jablon* (paragraph [0076]) further explains that "Alice may construct V_A using a one-way function of the value of K, since K is a one-time randomly-generated large value". *Jablon* thus teaches that the verification value V_A is constructed as the result of a one-way function of K, which is itself the result of a function whose input parameter is Q_B which is computed by Bob and sent to Alice from Bob.

In contrast, independent claim 1 recites that the authentication value is entirely or partly equal to the result of a serial function whose input parameters are at least the random number r and a private key s. *Jablon* fails to teach or suggest this recited feature of independent claim 1.

Moreover, independent method claim 1 recites the step of "verifying, at the application, said authentication value V via a verification function whose input parameters consist of public parameters including at least a public key p". *Jablon* also fails to teach or suggest this claimed step. As recited in claim 1, the input parameters of the verification function are public parameters. *Jablon*, on the other hand, teaches that the input parameter of verification function h(h) is K (see FIG. 1, 109 & 129), i.e., the input parameter is secret and is known only to Alice and Bob (where K can then be transformed into a secure authenticated session key). *Jablon* thus additionally fails to teach or suggest the subject matter of independent method claim 1 for this reason as well.

The Examiner cites *Yeda* in an effort to cure the shortcomings of *Jablon* and *Patarin*; specifically, the failure to teach or suggest "the producing of a pseudo-random number at application prior to a transaction, calculating a corresponding parameter x at the application prior to the transaction, and the parameter being linked to pseudo-random number r by a mathematical relationship and storing of parameter x in memory of chip prior to transaction".

The combination of *Jablon*, *Patarin* and *Yeda*, however, in fact fails to achieve the claimed invention, at least because (as discussed above) *Patarin* additionally fails to teach or suggest that a parameter x is previously calculated by the application and is stored in a data memory of the electronic chip, all prior to the transaction, as recited in now-amended independent claim 1.

Yeda relates to a method and apparatus for implementing an identification and signature scheme (see Abstract). According to *Yeda*, the method and apparatus "enable an entity to

generate proofs of identity and signatures of messages that everyone can verify but no one can forge" (see pg. 2, lines 12-13). Indeed, *Yeda* (Fig. 1, block 14) does disclose the production of a pseudo-random number. However, *Yeda* provides nothing to enable the skilled person to derive the method of independent claim 1 based on the production of this pseudo-random number. That is, *Yeda* fails to teach or suggest that a corresponding parameter x is calculated (i.e., at an application) prior to a transaction. Rather, *Yeda* (pg. 2, lines 44-45) explains that "[t]o prove his, hers or its identity, the entity chooses a random r in the range $0<r<n$, block 14, and sends $x=r^d$ (mod n) to the verifier, block 16 and line 18, where it is received by the verifier, block 20". *Yeda* thus clearly teaches that the parameter is not calculated prior to transaction but, rather, the parameter is calculated after choosing the random number from an in-process transaction.

Moreover, *Yeda* (pg. 3, lines 55-57) states that "[t]he size of the private key is about 4 kilobytes, but since each entity has to store only one such file, it can fit into almost any microcomputer based device (with the possible exception of a smart card)". This section of *Yeda* thus merely teaches that it — i.e., storage of the approximately 4 kilobyte private key — cannot fit into a smart card. This section of *Yeda* does not teach that a parameter x is stored in the memory of a chip.

In *Yeda*, the parameter is calculated by the prover (e.g., the chip) each time the chip is required to prove its identity via a mathematical expression $x=r^d$ (*mod n*) (see, e.g., Fig. 1, block 16 (compute $x = r^d$ (*mod n*)). In the instant claimed invention, however, the parameter x is read from memory each time the chip is required to authenticate itself. This could only be possible if the memory has been previously filled with the correct pseudo-random number r, in the manner recited in independent claim 1. As described at pg. 4, lines 1-14, the claimed invention provides an asymmetrical method of authentication that can be implemented in a hard-wired chip, such as

a chip in which the surface area of the silicon is extremely small, where the calculation logic is reduced to extremely basic hard-wired operations.

The skilled person would have no reason whatsoever to apply the teachings of *Yeda* to the method of *Jablon* and *Patrin*, absent impermissible hindsight analysis based on applicant's disclosure. Lacking the storage of the parameter x that is calculated by the application prior to the transaction and is stored in a data memory of an electronic chip, prior to the transaction, the deficiency of *Jablon* and *Patrin* is apparent.

Independent claim 1 is therefore not rendered obvious and unpatentable by the proffered combination of *Jablon*, *Patarin* and *Yeda*. Reconsideration and withdrawal of the rejection of claim 1 as unpatentable over the combination of *Jablon* with *Patarin* and *Yeda* under 35 U.S.C. §103 are accordingly deemed to be in order, and early notice to that effect is solicited.

Dependent Claims

In view of the patentability of independent claims 1 and 32 for the reasons presented above, each of dependent claims 2-31 is respectfully deemed to be patentable therewith over the prior art. Moreover, each of these claims includes features which serve to still further distinguish the claimed invention over the applied art.

Conclusion

Based on all of the above, applicant submits that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are once more solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned in order to facilitate an early resolution of any outstanding issues.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By _____

Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: August 11, 2008